REMARKS

A Request for a One Month Extension of Time is enclosed herewith along with the appropriate fee. Please charge any additional fees or credit any overpayment to our Deposit Account No. 19-1995. A duplicate copy of this letter is enclosed for that purpose.

Claims 1-32 were pending in the patent application. Claims 2 and 9 are cancelled herewith without prejudice.

Claims 16, 19, 25 and 30 were objected to, and have been amended herein to correct typo-graphical errors therein pointed out by the Patent Office. The specification was objected to, and has been amended herein to correct a typo-graphical error therein pointed out by the Patent Office. Marked-up versions of the amendments to the specification and claims, showing the changes, are enclosed. Claims 1 and 8 have been amended to include the limitation of transmitting the scrambled signal and said data signal to a receiver. No new matter has been added. Entry of the amendments is respectfully requested.

FIGS. 1 and 4 were objected to as not including "prior art" designation thereon. However, FIG. 1 does include such designation. Further, FIG. 4 shows a system in which aspects of the present invention are implemented, and an example is described on page 16, lines 6-15, of the specification. Therefore, it is not clear from the Office Action why FIGS. 1 and 4 are objected to. Clarification is respectfully requested.

Claims 1-32 were rejected. Claims 1, 6, 8 and 13 were rejected under 35 USC 102(e) as being anticipated by USPN 5,809,139 to Girod et al. (hereinafter "Girod"). Claims 15, 16 and 19 were rejected under 35 USC 102(e) as being anticipated by USPN 6,061,451 to Muratani et al. (hereinafter "Muratani"). Claims 2-5, 7, 9-12 and 14 were rejected under 35 USC 103(a) as being unpatentable over Girod in view of USPN 5,742,685 to Berson et al. (hereinafter "Berson"). Claims 17 and 18 were rejected under 35 USC 103(a) as being unpatentable over Muratani. Claims 20-24, 26, 28, 29 and 32 were rejected under 35 USC 103(a) as being unpatentable over Muratani in view of Schneier (Applied Cryptography) and USPN 6,249,866 to Brundrett et al. (hereinafter "Brundrett"). Rejection of the claims is respectfully traversed.

A. Rejection of Claims 1, 6, 8 and 13 under 35 USC 102(e)

Rejection of claims 1, 6, 8 and 13 under 35 USC 102(e) as being anticipated by Girod is respectfully traversed because the claims as amended include limitations not taught or suggested by Girod. For Example Claim 1 includes the limitation of "transmitting the scrambled signal and said data signal to a receiver". As the Patent Office also states, this limitation is not taught to suggested by Girod.

In the Office Action, the Patent Office suggests that in Col. 4, lines 9-12, Berson teaches appending a decryption key to a cryptogram in order to facilitate recovery of the encryption information. The Patent Office then states that, as such, it would have been obvious to facilitate removal of the watermark in Girod by including a frequency spreading signal with the transmitted data as taught by Berson.

However, Berson is non-analogous art. Berson is directed to an identification card and method and apparatus for producing and authenticating such an identification card. A person whom the identification card will identify, is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into one portion of the identification card. The image is also printed or otherwise embodied onto another portion of the identification card. In one embodiment, the signal representing the image is encrypted using a public key encryption system and the key is downloaded from a center. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. As such, Berson has nothing to do with the present invention.

Further, it is respectfully submitted that the Patent Office's interpretation of Berson is lacking. Nowhere in Berson are the limitations of "transmitting the scrambled signal and said data signal to a receiver" according to the present invention taught or suggested. In Col. 4, lines 1-41, Berson clearly states that image I and text T are embodied in card C in both humanly recognizable form on the front CF and coded and encrypted form on the back CB of card C. In a preferred embodiment (FIG. 1), a data center 40 transmits encryption code E_i to encrypter module 20. To facilitate decryption of encrypted information $E_i[M]$, data center 40 also transmits an encrypted decryption key $X[D_i]$ to be appended to the encrypted information $E_i[M]$ by coder module 22. When card C is to be verified, the necessary decryption key D_i can be obtained by decrypting encrypted decryption key $X[D_i]$.

As such, in Berson data center 40 sends encryption key E_i and decryption key D_i to encrypter module 20, such that the encrypted information $E_i[M]$ and decryption key D_i are placed on the card for later validation of the card. By contrast, according to the present invention, an audiovideo digital signal is first encoded to obtain an encoded signal, and the encoded signal is converted into a copy protected signal using a copy protection function (the copy protection function utilizes a CP data signal representing copy protection data). Then the copy protected signal is scrambled to obtain a scrambled signal; and the scrambled signal and said CP data signal are transmitted to a receiver. Simply put, in Berson an encryption key E_i and an encoded decryption key $X[D_i]$ are transferred from center 40 to encrypter module 20. In contrast, according to the claimed invention, a scrambled, copy protected, signal and, the CP data signal, are transmitted to the receiver. This difference is further shown by FIG. 2 of Berson which shows apparatus 50 for validating the identification card C. The back CB of card C is scanned by a barcode scanner 52 having the capability to scan an appropriate two dimensional barcode. The scanned signal is then decoded by decoder module 54 and decrypted by decrypter module 58. Key X (or keys) is obtained by decrypter 58 from center 40. According to Col. 4, lines 9-12 of Berson, the data center 40 does not send out copy protected, encrypted information, AND a data signal to be used to remove the copy protection. The data center only provides encryption and decryption keys to encrypter 20. This is totally different than the present invention.

Therefore, for at least the above reasons, amended Claim 1 is patentably distinct from the cited references, alone or in combination. Accordingly, rejection of Claim 1, and dependent claims therefrom, should be withdrawn. For the same reasons, rejection of amended Claim 8, and dependent claims therefrom, should be withdrawn. Further, the references, alone or in combination, do not teach limitations of claims 6 and 13. For example, neither of the references teaches or suggests reconverting the recovered copy protected signal back into said encoded signal using an inverse copy protection function, wherein the inverse function utilizes copy protection data from said copy protection data signal. The Patent Office's reliance on Girod is misplaced. Girod does not teach or suggest an inverse copy protection function that utilizes copy protection data from said copy protection data signal provided by a transmitter. Unlike the claimed invention herein, Girod does not offer the flexibility of using copy protection data to introduce copy protection, and then use the transmitted copy protection data, to recover/remove the copy protection. Nowhere in Girod, or other cited references, are such limitations taught or suggested. There is no teaching of a step or device for recovering and saving copy protection data that is then used by a reconverter to reconvert a copy protected signal. Nor are the other components of the copy protection system in the claims taught or suggested by the references, alone, or in combination. As such, rejection of the claims should be withdrawn.

B. Rejection of Claims 15, 16 and 19 under 35 USC 102(e)

Rejection of Claims 15, 16 and 19 under 35 USC 102(e) as being anticipated by Muratani is respectfully traversed because the claims include limitations not taught or suggested by

Muratani. For example, Muratani does not teach or suggest:

"a processor for: (i) removing said data signal from the digital signal, and storing the copy protection data represented by the data signal in a memory device, (ii) extracting said scrambled signal from the digital signal, and (iii) providing the scrambled signal to the descrambler via the link;" and

"a reconverter for converting an incoming copy protected signal from the descrambler back into said audiovisual signal using an inverse copy protection function, wherein the inverse function utilizes said stored copy protection data ..." (Claim 15).

Muratani is directed to a data receiving apparatus as a set top unit connected to a network and a security module. Digital video data which is supplied from the network and scrambled according to a first system is scrambled according to a second system in a scramble circuit in the set top unit, and is supplied to the security module. The data is descrambled according to the first system in a descramble circuit in the security module, and is transferred back to the set top unit. The data is descrambled according to the second system in a descramble circuit in the set top unit, and is outputted to an image display terminal.

The Patent Office's characterization of FIG. 2 of Muratani is lacking. Despite the Patent Office's characterization, in FIG. 2 and Col. 5, line 9 to Col. 6, line 11, Muratani teaches receiving a first scrambled signal (scrambled according to first scrambling system (Sa)), into a receiver (set top unit) 50. This first scrambled signal is input to demodulator 52, wherein an output of the receiver/demodulator 52 is supplied to the scramble circuit 54, which performs a second scramble process Sb different from the first scramble process Sa, and to the key control circuit 62 which controls a key of the second scramble process. When data is supplied from the receiver/demodulator 52 to the key control circuit 62, the key control circuit 62 generates the scramble key for the second scramble process Sa and corresponding descramble key, and supplies the scramble key and descramble key respectively to the scramble circuit 54 and the descramble circuit 56.

The double-scrambled signal is sent to security module 70, where it is once descrambled according to the first scrambling system (Da). Then, the once-descrambled signal is sent back to the receiver 50 where it is descrambled again in the descrambler circuit 56 according to the second scrambling system (Db), to obtain display data. As such, Muratani does not teach any of the above limitations. Further, The components in set-top unit 50 do not operate as the Patent Office represents. Muratani simply teaches receiving a scrambled signal (Sa) and then scrambling it again (Sb).

Therefore, there is no teaching in the references, alone, or in combination, of a system with the specified components, that receives copy protected signal and copy protection data as a single signal, and then (1) recovers copy protection data from the single signal, (2) recovers said copy protected data from the single signal, and (3) uses the recovered copy protection data to reconvert the copy protected data. The references, alone or in combination, do not teach or suggest a system according to the present invention that receives a single signal (i.e., an initial digital signal that is processed into an encoded, copy protected and scrambled signal (first signal) combined with a copy protection data signal (second signal) into the single signal), and then processes the received signal such that: (1) the copy protection data signal (second signal) is removed, (2) the scrambled signal (first signal) is recovered and descrambled to regain the copy protected signal, (3) the copy protected signal is reconverted to the encoded signal by inverse copy protection using the stored copy protection data, and (4) the encoded signal is decoded to recover said initial digital signal. For example, a processor 210 (or such a function) shown in FIG. 2 and described in the patent application, for removing the copy protection data signal (second signal) from the single signal, storing copy protection data represented by the copy protection data signal, and extracting the scrambled signal (second signal) from the single signal to provide to a descrambler (e.g., Claim 15(b)(2)) are not taught or suggested by the references, alone or in combination. The Patent Office's suggestion that a descrambler performs the same function as processor 210 is respectfully traversed, as clearly the processor 210 and a descrambler perform different functions as described above. Therefore, for at least the above reasons, it is respectfully requested that the rejection of Claim 15, and claims dependent therefrom, should be withdrawn.

C. Rejection of Claims 2-5, 7, 9-12 and 14 under 35 USC 103(a)

Claims 2-5, 7, 9-12 and 14 were rejected under 35 USC 103(a) as being unpatentable over Girod in view of Berson. Rejection of the claims are respectfully traversed because the claims include limitations not taught or suggested Girod or Berson, alone or in combination. For example, the limitations of transmitting the scrambled signal and the CP data signal as a single signal (Claims 3, 10) and combining the two signal as a single signal (Claims 4, 11), are not taught or suggested by the references, alone or combination. Further, for example, limitations in parts (a)-(d) of Claim 5, parts (a)-(e) of Claim 7, parts (a)-(d) of Claim 12, and parts (a)-(c) of Claim 14, are not taught or suggested by the references, alone or combination. The Patent Office has not shown where these limitations are disclosed in the references. For at least these reasons and the reasons provided above in sections A and B, rejection of the claims should be withdrawn.

D. Rejection of Claims 17 and 18 under 35 USC 103(a)

Claims 17 and 18 were rejected under 35 USC 103(a) as being unpatentable over Muratani. The rejection of Claims 17 and 18 is respectfully traversed, because as the Patent Office also states Muratani does not teach or suggest PCMCIA or IS679 as claimed. Muratani's only reference to use an IC is not a teaching to use PCMCIA or IS679. No motivation, suggestion or teaching is provided in Muratani or other references to use such features, nor has the Patent Office provided such. Therefore, it is respectfully submitted that rejection of claims 17 and 18, should be withdrawn.

E. Rejection of Claims 20-24, 26, 28, 29 and 32 under 35 USC 103(a)

Claims 20-24, 26, 28, 29 and 32 were rejected under 35 USC 103(a) as being unpatentable over Muratani in view of Schneier and Brundrett. The rejection of the claims is respectfully traversed because the claims include limitations not taught or suggested by the references, alone or in combination. Such limitations include, for example: receiving a scrambled audio-visual digital signal in a receiver, transmitting the scrambled digital signal to a descrambler module and descrambling the scrambled digital signal in the descrambler module to generate a descrambled signal, generating a copy protection data signal and converting the descrambled signal into a copy protected signal in the descrambler module using the copy protection data signal. Then sending the copy protected signal from the descrambler module to the receiver, where it is reconverted to the audio-visual signal by an inverse copy protection function using the copy protection data signal.

The Patent Office's characterization of Muratani (e.g., FIG. 2) is lacking for the reasons provided in section B above, and incorporated herein by reference. Further, despite the Patent Office's contention, the key control circuit 62 does not satisfy limitations of clause (b) of Claim 20. Muratani specifically states in Col. 5, line 9 to Col. 6, line 11, that when data is supplied from the receiver/demodulator 52 to the key control circuit 62, the key control circuit 62 generates the scramble key for the second scramble process and corresponding descramble key, and supplies the scramble key and descramble key respectively to the scramble circuit 54 and the descramble circuit 56. Therefore, despite the Patent Office's interpretation, key control circuit 62 does not generate copy protection data and as such does not meet limitations of part (b) of Claim 20.

Muratani does not meet limitations of part (c) of Claim 20, because Muratani sends a twice-scrambled signal to module 70 in FIG. 2. This is because the incoming scrambled signal, is scrambled again in scramble circuit 54.

Muratani does not meet limitations of part (d) of Claim 20, because descrambling said twice-scrambled signal in descramble circuit 72, still provides a one-scrambled signal, and not the audio-video signal as claimed Specifically, circuit 72 (Da) removes scrambling Sa, such that signal output of circuit 72 is still scrambled according to scramble circuit 54 (Sb).

As the Patent Office also states, Muratani does not meet limitations of part (e) of Claim 20. Further, Muratani does not meet limitations of parts (f) and (g) of Claim 20. No copy protected data is transferred anywhere in Muratani at all. There is no copy protection using copy protection data as claimed, taught or suggested anywhere in Muratani. There is no inverse copy protection function in Muratani. Applicant respectfully requests that the Patent Office specifically point to such teachings or suggestions in Muratani. What is returned from module 70 to unit 50 is a scrambled signal, not transmitting a copy protected signal using copy protection data, as claimed in part (f) of Claim 20. Descrambling in element 56 is not reconverting the copy protected signal to the audio-visual signal in the receiver using an inverse copy protection function, wherein the inverse function utilizes the data signal that represents said copy protection data, as claimed in part (g) of Claim 20

Nor are limitations of Claim 20 taught or suggested in the other references, alone or in combination. Brundrett is directed to a system and method for encryption and decryption of files. In its Background section, Brundrett discusses existing problems where users tend to lose their keys to decrypt encrypted files. Brundrett states that the problem of lost keys can be eliminated by spreading the key around to multiple users, but this further compromises security. Moreover, each file may have a different password, making recall difficult. Accordingly, for convenience many users will encrypt many files with the same password key used to encrypt one file, whereby divulging a key to another person for one file often results in inadvertently giving that person the key to many other files. Moreover, in order to remove or add user access to one or more files, each file (and every copy of each file) must be decrypted and re-encrypted with the new key, and then redistributed (Col. 1, lines 39-50).

The Patent Office provides simply states that it would have been obvious to maintain security in transmissions between the set top unit and security module while avoiding miscommunication causes by non-commutative algorithms by decrypting data in the security mode and then re-encrypting it with a key known to the recipient (the set tip box in this case) as shown in Brundrett.

The Patent Office is interpreting the sentence in Col. 1, lines 47-50 of Brundrett to evidently teach the limitations in parts (e) and (g) of Claim 20. This interpretation is respectfully traversed. All Brundrett does is mention that in order to remove or add user access to one or more files, each encrypted file must be decrypted and re-encrypted with the new key, and then redistributed. Further, it is respectfully submitted that such process is different than the claimed process of: receiving a scrambled audio-visual digital signal in a receiver, transmitting the scrambled digital signal to a descrambler module and descrambling the scrambled digital signal in the descrambler module to generate a descrambled signal, generating a copy protection data signal and converting the descrambled signal into a copy protected signal in the descrambler module using the copy protection data signal, and then sending the copy protected signal from the descrambler module to the receiver, where it is reconverted to the audio-visual signal by an inverse copy protection function using the copy protection data signal. The Patent Office has not explained how these processes are similar.

Further, Muratani cannot be modified as the Patent Office confusingly suggests. In Muratani, despite the Patent Office's suggestion, there is no copy protection function, scrambling or encryption of any sort taking place in the security module 70. The module 70 only descrambles a scrambled signal provided to it by the receiver 50. And, in Muratani, the same receiver 50 provides encryption keys (circuit 62), and performs the symmetric scrambling (circuit 54) and descrambling (circuit 56) functions using the encryption keys from circuit 62, therein. Whereas in Claim 20 herein, shown by example 3 in FIG. 3, the receiver 302 performs no scrambling of the incoming signal. Rather, the incoming signal is routed to the descrambler module304 where it is descrambled by a descrambler circuit 308. Further, although the receiver 302 generates the copy protection data signal, that data signal is provided to the descrambler module 304 to perform the copy protection function (F) on the descrambled signal therein. Then, the copy protected signal is routed to the receiver 302, wherein the inverse copy protection function is performed using the copy protection data signal. In Muratani, the signal passed from receiver 50 to the module 70 is first scrambled by circuit 54 in the receiver 50. Whereas in the claimed invention, the signal from the receiver to the descrambler is not scrambled in the receiver before being passed to the descrambler module.

As described above, despite the Patent Office's suggestion, key control circuit 62 in FIG. 2 of Muratani does not provide copy protection data as claimed in Claim 21. Further, the limitation in Claim 22 if generating copy protection data in the receiver and transmitting to the descrambler is important is not taught or suggested, and is needed to allow the descrambler to copy protect the descrambled signal to send to the receiver in a protected manner. Unlike the claimed invention, no copy protection data is provided from element 62 to module 70 in FIG. 2 of Muratani to copy protect data.

Rejection of claims 25, 27, 30 and 31 on the same grounds as claims 17 and 18 is respectfully traversed for at least reasons detailed above in support of claims 17 and 18. Therefore, rejection of claims 25, 27, 30 and 31 should be withdrawn.

There is no motivation or suggestion in any of the cited references to combine them. One of ordinary skill in the art would not look to the references for the features of the claimed invention. One of ordinary skill in the art cannot combine the references to achieve the features of the claimed invention, because as detailed above, any unlikely combination would not teach or suggest limitations of the claimed invention. Further, Muratani's system cannot be modified according to Brundrett as it has no capability for copy protection, nor does it require such. Further, Brundrett is non-analogous art because it is directed to file protection in a network, not transmission of audio-visual information and copy protection such as watermarking.

For these, and other reasons, it is believed that the claims are allowable.

Respectfully submitted,

SHERMAN & SHERMAN

10/3/02

Kenneth L. Sherman
Registration No. 33,783
2029 Century Park East
Seventeenth Floor
Los Angeles, CA 90067
Telephone: (310) 789-3200
Facsimile: (310) 789-3210

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service first class mail in an envelope addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231 on October 3, 2002.

Evelyn Menjivar
(Type or print name of person mailing paper)

Evelyn M
(Signature of person mailing paper)

G:\KLS\SAM1\SAM10058\02AMD.doc

Marked-up version of the Amended Specification Paragraphs and Amended Claims

In the Specification, amend paragraph on lines 10-21 on page 5 as follows:

After receiving the single audio-visual signal, receiver 106 transmits the audio-visual signal to a replaceable security module 110 via an interface 112. For IS679 applications, replaceable security module 110 is a smart card or a PCMCIA card that is communicatively coupled to receiver 106 via an IS679 compatible interface 112. However, other types of interfaces may also be used to couple replaceable security module 110 to receiver 106. Replaceable security module 110 includes a [de-scrambles] de-scrambler 114 that removes the encryption placed into the encoded audio signals AS_1, AS_2 through AS_N and video signals VS_1, VS_2 through VS_N by scramblers S_1, S_2 through S_N. The de-scrambled single audio-visual signal is then returned to receiver 106 and decoded with a decoder 116 contained in receiver 106. The de-scrambled and decoded audio-visual signal is then provided to a display 118 to be displayed or otherwise viewed.

Please amend the claims as follows:

1. (Amended) A method of copy protecting a digital signal representing audiovisual information, comprising the steps of:

(a) encoding the digital signal to obtain an encoded signal;

(b) converting the encoded signal into a copy protected signal using a copy protection function, wherein the function utilizes a data signal representing copy protection data; [and]

(c) scrambling the copy protected signal to obtain a scrambled signal; and

(d) transmitting the scrambled signal and said data signal to a receiver.

Please cancel claim 2 without prejudice.

8. (Amended) A system for copy protecting a digital signal representing audiovisual information, comprising:

(a) an encoder to encode the digital signal to obtain an encoded signal;

(b) a converter to convert the encoded signal into a copy protected signal using a copy protection function, wherein the function utilizes a data signal representing copy protection data; [and]

(c) a scrambler for scrambling the copy protected signal into a scrambled signal; and

(d) a transmitter for transmitting the scrambled signal and the data signal to a receiver.

Please cancel claim 9 without prejudice.

17. (Amended) The system of claim 15, wherein the descrambler module comprises a [PCMIA] PCMCIA card.

19. (Amended) The system of claim [215] 15, wherein the link comprises one or more communication mediums configured for carrying audio-visual signals.

25. (Amended) The method of claim 20, wherein the descrambler module comprises a [PCMIA] PCMCIA card.

30. (Amended) The system of claim 28, wherein the descrambler module comprises a [PCMIA] PCMCIA card